WHAT IS CLAIMED IS:

Sub D1 1. A method of facilitating verifiable gaming transactions in a distributed environment, the method comprising:

executing nested first- and second-type commit/reveal sequences, wherein the first-type commit/reveal sequence commits an outcome generator to a set of outcomes, and instances of the second-type commit/reveal sequence commit at least each player to a respective index contribution and only thereafter reveal the respective index contributions;

selecting from the set of outcomes based on a predefined combination operation on the index contributions; and

thereafter revealing the set of outcomes for validation thereof.

2. The method of claim 1,

wherein the set of outcomes correspond to card values from one or more decks thereof.

3. The method of claim 2,

wherein the cards values are shuffled.

4. The method of claim 2,

wherein the card values are unshuffled, but the predefined combination operation further operates on an index contribution of the outcome generator.

5. The method of claim 1, wherein the set of outcomes correspond to a set of values at least partially defined by one or more of:

a deck of cards;

sides of a die;

sides of a coin; and

slots of a wheel.

6. The method of claim 1, wherein the first-type commit/reveal sequence includes:

encryption of the set of outcomes;

supply of the encrypted set of outcomes to each of the players; and

later access to set of outcomes using a key.

7. The method of claim 1, wherein the first-type commit/reveal sequence includes:

encryption of individual ones of the outcomes;

supply of the ordered set of encrypted outcomes to each of the players; and

later access to the selected outcomes using respective keys.

8. The method of claim 1, wherein the second-type commit/reveal sequence includes:

hashing of respective index contribution using a predetermined hash;

supply of the hashed index contributions to the outcome generator and to all of the players; and

later supply of the index contributions to the outcome generator and to all of the players.

9. The method of claim 1,

wherein the first- and second-type commit/reveal sequences include respective transformational securings selected from the set of cryptographic encodings, hashes and irreversible transforms.

10. The method of claim 1,

wherein the first-type commit/reveal sequence is performed substantially by a game processor; and

wherein the second-type commit/reveal sequence is performed substantially by respective player processors.

11. A verifiable gaming transactions method comprising:

transformationally securing an encoding of a predetermined set of outcomes;

supplying one or more players with the transformationally secured encoding;

receiving a transformationally secured player index from each of the one or more players; and selecting a particular one of the outcomes for revealing to the one or more players based on a combination of the player indices.

12. The method of claim 11,
wherein the predetermined set of outcomes is transformationally secured using a cryptographic key; and
wherein the player indices are transformationally secured using a hash.

13. The method of claim 11, further comprising:
receiving and verifying the player indices against respective transformationally secured player indices prior to the outcome selecting.

14. The method of claim 11, further comprising:
randomizing ordering of the predetermined set of outcomes prior to the securing thereof.

Sub B1 15. The method of claim 11, further comprising:
effectively randomizing the set of outcomes by further combining the player indices with the randomized index.

16. The method of claim 11,
wherein the combination includes a bit-wise exclusive OR of binary encodings of the player indices.

17. The method of claim 11,
wherein the selecting includes a modulo function.

Sub B2 18. The method of claim 11,
wherein the transformational securing of the randomized set encoding includes cryptographically securing the set of outcomes.

19. The method of claim 11,

wherein the transformational securing of the randomized set encoding includes cryptographically securing individual outcomes of the set thereof.

20. A verifiable gaming transactions method comprising:
receiving a transformationally secured encoding of a predetermined set of outcomes for a gaming transaction;
supplying a transformationally secured encoding of a player input;
after each of zero or more other participants in the gaming transaction has supplied a transformationally secured corresponding input, supplying the player input; and
accessing a particular one of the outcomes selected based on a combination of the player input with the corresponding input for each of the zero or more other participants.

21. The method of claim 20, further comprising:
supplying successive player inputs after prior supply and receipt of corresponding transformationally secured inputs; and
accessing successive one of the outcomes selected based on combination of the successively supplied player inputs with the corresponding inputs for each of the zero or more other participants.

22. The method of claim 20,
wherein the accessing includes receiving an encoding of the particular outcome subject to later verification against the transformationally secured set of outcomes.

23. The method of claim 20,
wherein outcomes of the transformationally secured set thereof are individually secured; and
wherein the accessing includes obtaining a key for a corresponding individually secured outcome.

Sub B37

24. The method of claim 20,

wherein outcomes of the transformationally secured set thereof are individually secured; and

wherein the accessing includes receiving an encoding of the particular outcome for verification against the corresponding individually secured outcome.

25. An outcomes generator for verifiable gaming transactions comprising:

a commitment sequence executable to supply one or more players with a transformationally secured set of outcomes; and

a reveal sequence responsive to receipt of transformationally secured player index contributions from each of the one or more players, the reveal sequence executable to select a particular one of the outcomes based on a combination of the player indices.

26. The outcomes generator of claim 25,

integrated with, and responsive to, game logic.

27. The outcomes generator of claim 25,

wherein the commitment and reveal sequences employ cryptographic transformations.

28. A player client for verifiable gaming transactions comprising:

a commitment sequence executable, after receipt of a transformationally secured encoding of a predetermined set of outcomes, to supplying a transformationally secured encoding of a player input; and

a reveal sequence executable, after each of zero or more other participants in a gaming transaction has supplied a transformationally secured corresponding input, to reveal the player input; and

a selector for a particular one of the outcomes based on a combination of the player input with the corresponding input for each of the zero or more other participants.

29. A computer program product encoded in one or more computer readable media and comprising:

first instructions executable by a computing machine as part of a first commit/reveal protocol to supply one or more players with a transformationally secured set of outcomes;

second instructions executable by the computing machine to distribute transformationally secured player index contributions from each of the one or more players and only thereafter distribute the index contributions as part of a second commit/reveal protocol nested within the first commit/reveal protocol; and

third instructions executable by the computing machine to reveal the set of outcomes.

30. The computer program product of claim 29,

wherein the one or more computer readable media are selected from the set of a disk, tape or other magnetic, optical, or electronic storage medium and a network, wireline, wireless or other communications medium.

31. A method of making a computer-readable encoding of a verifiable gaming outcome, the method comprising:

transformationally securing an encoding of a predetermined set of outcomes;

supplying one or more players with the transformationally secured encoding;

receiving a transformationally secured player index from each of the one or more players;

selecting a particular one of the outcomes for revealing to the one or more players based on a combination of the player indices; and

encoding as the computer-readable encoding, information usable by the one or more players to reveal the selected outcome.

Sub B47

32. The method of claim 1,

wherein the information encodes the selected outcome.

33. The method of claim 1,

wherein the information includes a key to reveal at least the selected one of the outcomes from the supplied transformationally secured encoding thereof.

34. The method of claim 1,
wherein the computer-readable encoding includes at least one message suitable for communication between a gaming server and a client thereof.

35. An apparatus comprising:
means for committing to a particular set of outcomes without revealing same; and
means for ensuring an irrevocable commitment to respective index contributions by each party to a distributed transaction and only thereafter revealing a particular one of the outcomes based on a combination of the index contributions.

Add C1